Introduction to the Common Criteria for IT Security (ISO 15408)

Common Criteria

Gene Troy

US National Institute of Standards
and Technology (NIST)

Fuji Xerox Co. & Keio University
March 1999

Overview

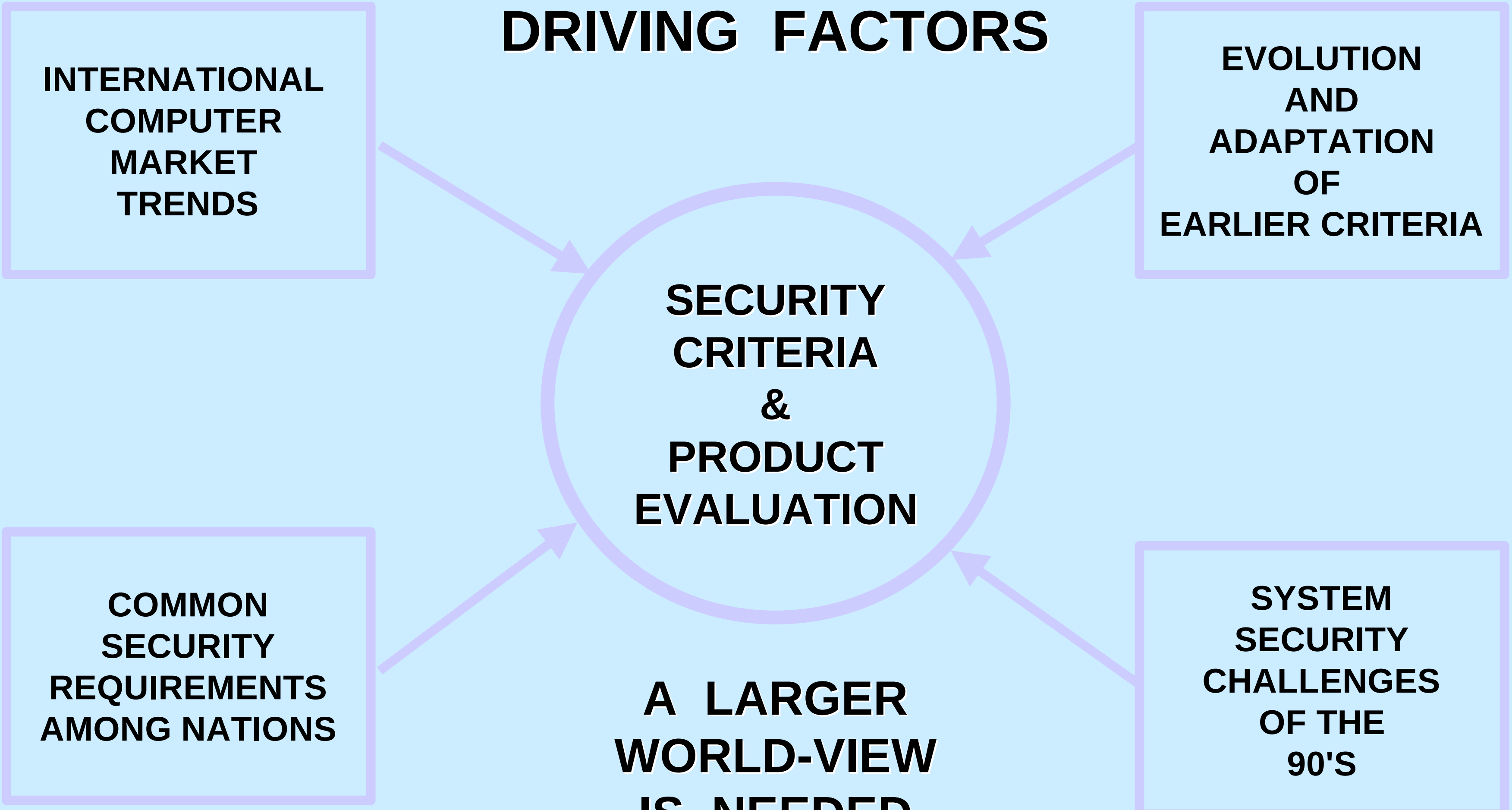
- **Introduction**
  - **What are IT Security Criteria & why do we need them?**
  - **What are the goals of the Common Criteria Project?**
- **The Common Criteria (CC), its organization & contents**
- **Using the CC in product evaluations**
- **Implementing the CC world-wide**
- **Japanese implementation of the CC**

Introduction

What are IT Security Criteria?

- (User view) A way to define Information Technology (IT) security requirements for some IT products:
  - Hardware
  - Software
  - Combinations of above
- (Developer view) A way to describe security capabilities of their specific product
- (Evaluator/scheme view) A tool to measure the confidence we may place in the security of a product.

The Common Criteria
-- WHY DO IT?



DRIVING FACTORS

INTERNATIONAL
COMPUTER
MARKET
TRENDS

EVOLUTION
AND
ADAPTATION
OF
EARLIER CRITERIA

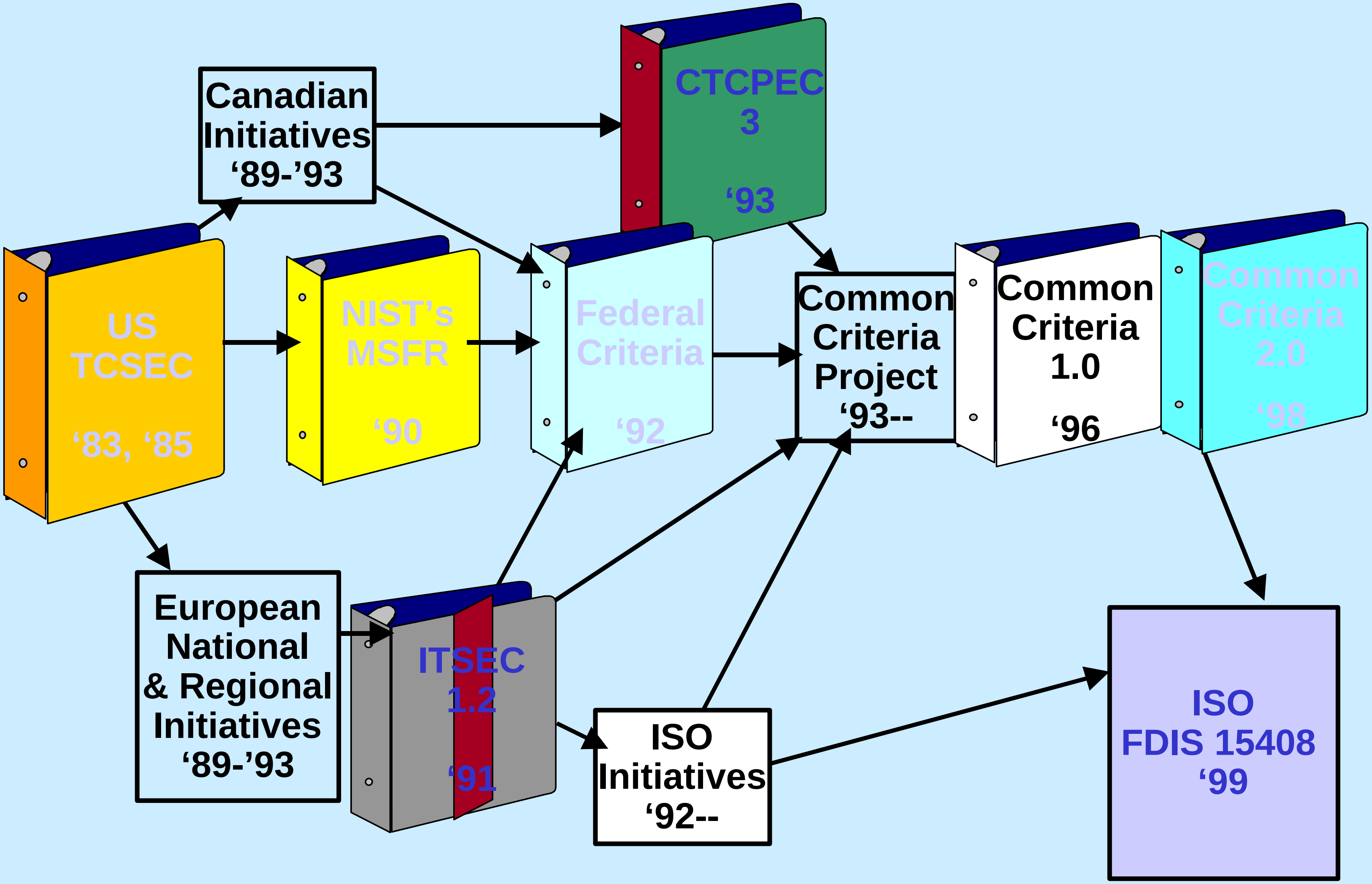
SECURITY
CRITERIA
&
PRODUCT
EVALUATION

COMMON
SECURITY
REQUIREMENTS
AMONG NATIONS

SYSTEM
SECURITY
CHALLENGES
OF THE
90'S

A LARGER
WORLD-VIEW
IS NEEDED

History of IT Security Criteria



Canadian Initiatives ‘89-’93

CTCPEC 3 ‘93

US TCSEC ‘83, ‘85

NIST’s MSFR ‘90

Federal Criteria ‘92

Common Criteria Project ‘93--

Common Criteria 1.0 ‘96

Common Criteria 2.0 ‘98

European National & Regional Initiatives ‘89-’93

ITSEC 1.2 ‘91

ISO Initiatives ‘92--

ISO FDIS 15408 ‘99

Goals of CC Project

- Single international (common) IT product & system security criteria -- the CC
- CC becomes ISO International Standard 15408
- International mutual recognition of product evaluations -- Agreement is now in place
- Level international playing field for developers
- Better world-wide availability of IT security-capable products

The Common Criteria (CC), its organization & contents

What IS the Common Criteria ??

What the Common Criteria is --

- ➢ Common structure & language for expressing product/system IT security requirements (Part 1)
- ➢ Catalogs of standardized IT security requirement components & packages (Parts 2 & 3)

How the CC is used --

- ➢ Develop Protection Profiles and Security Targets -- specific IT security requirements for products & systems -- *Consumers then use them for decisions*
- ➢ Evaluate products & systems against known & understood requirements => CONFIDENCE

More on Using the CC

Individual IT Product Consumers --

- Look for PPs matching your security requirements -- use in procurement specifications

Consumer Consortia (Users Groups) --

- Use CC to build PPs expressing members’ needs
- Work with Product Developers to build matching products

Product Developers --

- Use CC to specify product security capabilities via Security Targets

Product Evaluators/Validators --

- Use CC-compliant Protection Profiles & Security Targets as yardstick for measuring product compliance

Key CC Concepts (1)

The CC defines two types of IT Security Requirements:

<u>Functional Requirements</u>

- for defining security behavior of the IT product or system:

- **implemented requirements become security functions**

(what a product does)

<u>Assurance Requirements</u>

- for establishing confidence in Security Functions:

- **correctness of implementation**
- **effectiveness in satisfying objectives**

(is the product built well & does it meet the purpose)

Key Concepts (2)
-- The Constructs

- **Protection Profile (PP):**
  An implementation-independent set of security objectives and requirements for a category of IT products or systems that meet similar consumer needs for IT security.
  - ***Examples: Firewall-PP, C2-PP, RBAC-PP***

- **Security Target (ST):**
  A set of security requirements and specifications for an identified IT product or system (the "Target Of Evaluation") -- to be used as the basis for its evaluation.
  - ***Examples: ST for Oracle v7, ST for MilkyWay Firewall***

Key Concepts (3)
-- About the "TOE"

- **Target of Evaluation (TOE):**

  An IT product or system that is the subject of an evaluation.

- **TOE Security Policy (TSP):**

  The rules that regulate how assets are managed, protected and distributed within a TOE.

- **TOE Security Functions (TSF):**

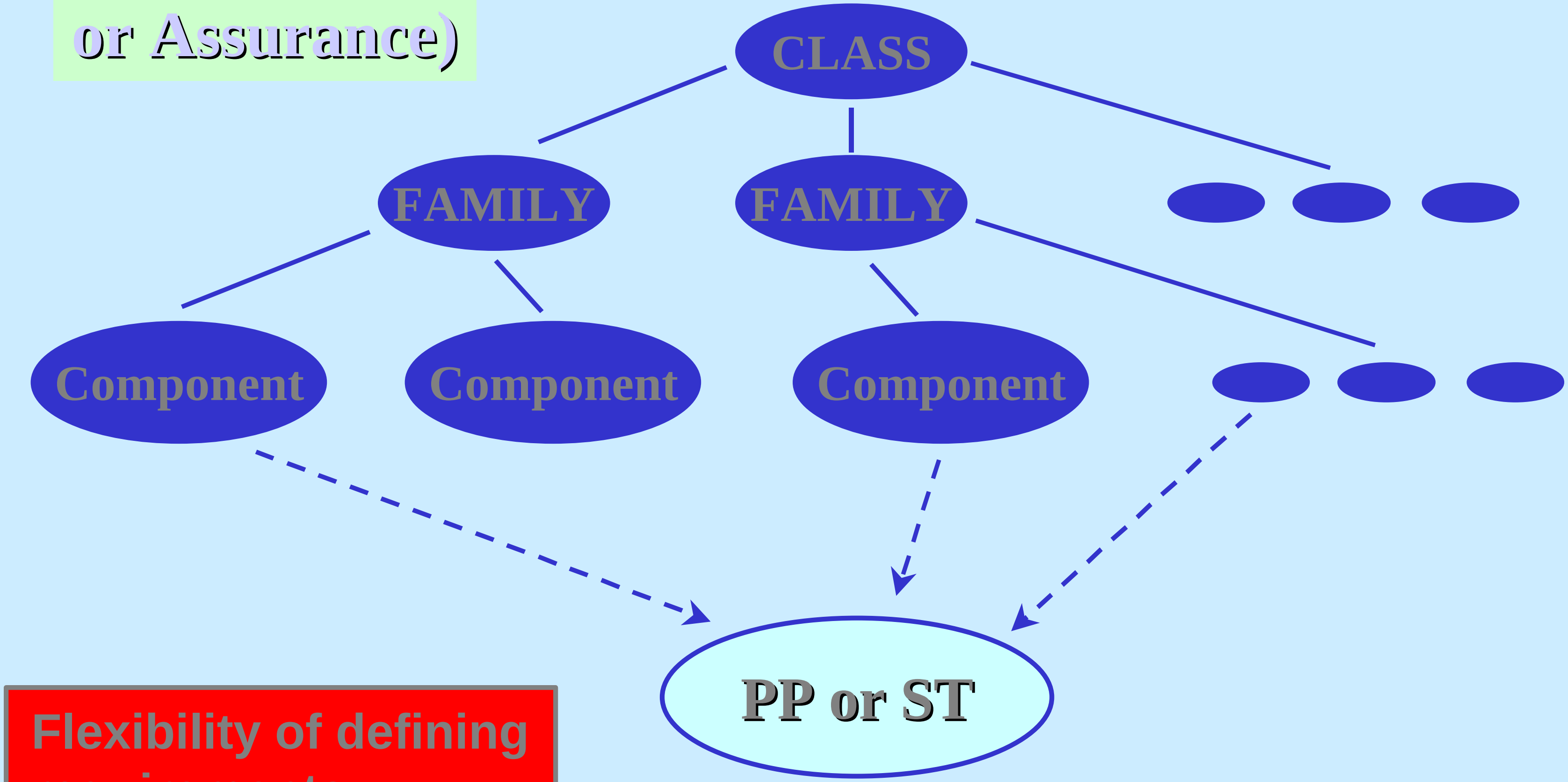
  All parts of the TOE that must be relied upon for the correct enforcement of the TSP.

Key Concepts (4)
Hierarchy of the Parts

- **CC functional / assurance hierarchy:**
  a set of constructs that classify security requirement components into related sets:
  - **Class (e.g. FDP - User Data Protection):**
    a grouping of families that share a common focus.
  - **Family (e.g. FDP_ACC - Access Control Policy):**
    a grouping of components that share security objectives but may differ in emphasis or rigor.
  - **Component (e.g. FDP_ACC.1 - Subset Access Control):**
    the smallest selectable set of elements that may be included in a PP / ST / package.

Example Hierarchy

(Functional or Assurance)



CLASS

FAMILY

FAMILY

Component

Component

Component

PP or ST

Flexibility of defining requirements.

CC Part 2 -- Catalog

- **Classes of Security Functional Requirements:**

Class	Name
FAU	Audit
FCO	Communications
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification & Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of TOE Security Functions
FRU	Resource Utilization
FTA	TOE Access
FTP	Trusted Path / Channels

CC Part 3 -- Catalog

- **Classes of Security Assurance Requirements:**

Class	Name
ACM	Configuration Management
ADO	Delivery & Operation
ADV	Development
AGD	Guidance Documents
ALC	Life Cycle Support
ATE	Tests
AVA	Vulnerability Assessment
APE	Protection Profile Evaluation
ASE	Security Target Evaluation
AMA	Maintenance of Assurance

Evaluation Assurance Levels (EALs)

(Basis for Mutual Recognition)

- **Evaluation Assurance Levels & (*rough*) Backward Compatibility Comparison**

EAL	Name	*TCSEC
EAL1	Functionally Tested	
EAL2	Structurally Tested	C1
EAL3	Methodically Tested & Checked	C2
EAL4	Methodically Designed, Tested & Reviewed	B1
EAL5	Semiformally Designed & Tested	B2
EAL6	Semiformally Verified Design & Tested	B3
EAL7	Formally Verified Design & Tested	A1

***TCSEC = “Trusted Computer Security Evaluation Criteria” -- ”Orange Book”**

Protection Profiles (generic)
& Security Targets (specific)

Protection Profile contents

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational Security Policies
- Security Objectives
- Security Requirements
  - Functional Req’ts
  - Assurance Req’ts
- Rationale

Security Target contents

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational Security Policies
- Security Objectives
- Security Requirements
  - Functional Req’ts
  - Assurance Req’ts
- *TOE Summary Specification*
- *PP Claims*
- Rationale

Protection Profiles
(Some Examples)

- **Operating Systems (C2, B1, CS2, RBAC)**
- **Database Management Systems (C.DBMS, G.DBMS)**
- **Firewalls (Packet Filter and Application)**
- **Smartcards**
- **Application Software, e.g.:**
    - **Electronic financial transaction (gov’t)**
    - **Credit card payment (customer / guarantor)**
    - **Accounting “bought ledger”**

Common Criteria
-- Current Status

- **Current Version:**
  - **CC version 2.0, May 1998 + 10/98 ISO tweaks**
  - **Now Called:**

ISO Final Draft International Standard 15408

- **Future Plans:**
  - **ISO balloting for final International Standard 15408 -- expected completion: 6/99**
  - **<u>CC Interpretations Management Board</u> (CCIMB) now established to interpret CC & maintain in future**

Using the CC
in Product Evaluations

CC Evaluation

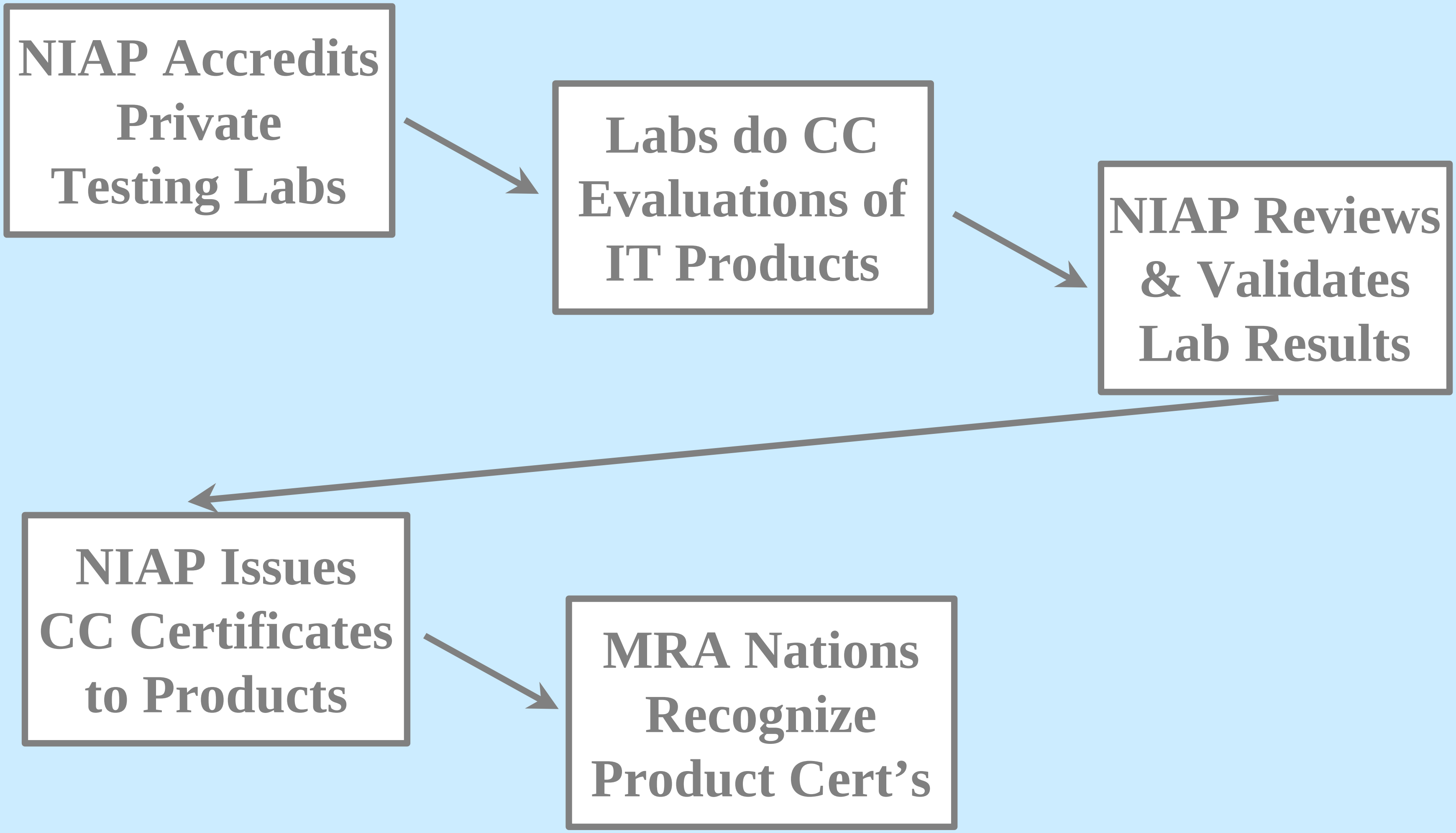
Approach to Evaluation under CC/15408:

- Protection Profile evaluation (Part 3 - APE)
- Product / system evaluation (two phases):
  - Security Target evaluation (Part 3 - ASE)
  - TOE evaluation (uses evaluated ST as baseline)

The CC Evaluation Scheme

- **Evaluation of IT security products under the CC is done within an "Evaluation Scheme" (agreed approach) by accredited laboratories.**
- **Laboratory evaluation work is under the oversight of an Evaluation Authority**
- **The Evaluation Authority issues a certificate upon successful completion of an evaluation**
- **In the U.S., the Scheme is called "NIAP" - National Information Assurance Partnership (NIST & NSA)**
- **NIAP is a partner in the international Mutual Recognition Arrangement (MRA)**

US Evaluation Scheme
-- Overview



NIAP Accredits Private Testing Labs

Labs do CC Evaluations of IT Products

NIAP Reviews & Validates Lab Results

NIAP Issues CC Certificates to Products

MRA Nations Recognize Product Cert’s

Common Evaluation Methodology (CEM)

What is the Common Evaluation Methodology?

- ➢CEM is a *necessary companion* to the CC.
- ➢CEM explains the *actions* evaluators must take to determine that CC requirements have been complied with.
- ➢CEM is used by evaluation schemes to ensure *consistent application* of CC requirements across multiple evaluations and multiple schemes.
- ➢Therefore, CEM is an important component of international mutual recognition.

CEM --
Release Schedule

- Part 1: Introduction & General Model
  - draft out for review (1/97)
- Part 2: Evaluation Methodology
  - PPs (APE) & STs (ASE): draft now out for review
  - EAL1-EAL4: draft now out for review
  - EAL5-EAL7: no schedule yet
- Part 3: Extensions to Methodology
  - No schedule yet

(See NIST's CC website for draft CEM review postings -- http://csrc.nist.gov/cc/cem/cemlist.htm)

Implementing the CC world-wide

Mutual Recognition of Product Evaluations

Common Criteria Mutual Recognition Arrangement --

- ➢ **Five nations now members: Canada, France, Germany, United Kingdom, United States**
- ➢ **IT security evaluations conducted by US testing laboratories recognized by the other nations**
- ➢ **Eliminates duplicate, costly security evaluations for product developers**
- ➢ **More nations to be added in near future**
- ➢ **New binding agreement to be negotiated in near future to expand recognition worldwide**

Japanese Implementation of the CC/ISO 15408

Security Evaluation Activities in Japan

- **Earlier JEIDA work**
  - ISO SC27 WG3 (since '91)
  - Minimum Security Functional Requirements ('94 & '97)
  - ECMA TC36 liaison (since '93)
  - Study of Evaluation Methodologies in US & UK (since '96)

Source: Mr. Haruki Tabuchi
IPA Task Force
(NAB03374@nifty.ne.jp)

- **Recent Activities**
  - Organization of Information Technology Promotion Agency (IPA) Task Force (3/98)
  - IPA Translation of CC into Japanese (6/98)
  - Production of various Guides
  - Trial Evaluations of products
  - Development of Tools for Developers & Evaluators
  - CS2-PP translation, study & evaluation (Seminar 3/23/98)

CC Contact Information

For more introductory info about the CC:

- **NIST-ITL Bulletin (11/98) , get it at: http://csrc.nist.gov/cc/info/cc_bulletin.htm**

To obtain an electronic copy of the CC:

- **Japanese: http://www.ipa.go.jp/SECURITY/ccj**
- **English: http://csrc.nist.gov/cc/ccv20/ccv2list.htm**

To get sample Protection Profiles:

http:/csrc.nist.gov/cc/pp/pplist.htm

For further information on the CC, contact:

➢ **Eugene F. (Gene) Troy, NIST/ITL**
email: eugene.troy@nist.gov Tel: +1.301.975.3361

Thank you very much for your kind attention and interest!

Domo arigato